TELKOMNIKA, Vol.17, No.3, June 2019, pp.1168~1175
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v17i3.12230

Hiding data in images using steganography techniques with compression algorithms

Osama F. AbdelWahab*[1], Aziza I. Hussein[2], Hesham F. A. Hamed[3], Hamdy M. Kelash[4], Ashraf A.M. Khalaf[5], Hanafy M. Ali[6]
[1,2,3,5,6]Faculty of Engineering, Minia University, El Minia, Egypt
[2]Electrical & Computer Eng. Dept., Effat University, Jeddah, KSA
[4]Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt
*Corresponding author, e-mail: osamaf@hotmail.com[1], azibrahim@effatuniversity.edu.sa[2]

Abstract

Steganography is the science and art of secret communication between two sides that attempt to hide the content of the message. It is the science of embedding information into the cover image without causing a loss in the cover image after embedding.Steganography is the art and technology of writing hidden messages in such a manner that no person, apart from the sender and supposed recipient, suspects the lifestyles of the message. It is gaining huge attention these days as it does now not attract attention to its information's existence. In this paper, a comparison of two different techniques is given. The first technique used Least Significant Bit (LSB) with no encryption and no compression. In the second technique, the secret message is encrypted first then LSB technique is applied. Moreover, Discrete Cosine Transform (DCT) is used to transform the image into the frequency domain. The LSB algorithm is implemented in spatial domain in which the payload bits are inserted into the least significant bits of cover image to develop the stego-image while DCT algorithm is implemented in frequency domain in which the stego-image is transformed from spatial domain to the frequency domain and the payload bits are inserted into the frequency components of the cover image.The performance of these two techniques is evaluated on the basis of the parameters MSE and PSNR.

Keywords*: DCT, LSB, MSE, PSNR, steganography, stego-image*

1. Introduction

The development of computer and the fast growth of internet usage over high bandwidth and low cost computer hardware to control the quickly growth of the steganography.In the recent years, hidden and secure communication is the primary requirement of people. Therefore, steganography is achieving attraction by people caused by the security issues over the internet. Steganography has retreated a digital strategy of hiding a file in some form of multimedia, such as an image, an audio/video files [1, 2]. The aim of steganography is hiding the embedded information in the cover image. Cryptography convert secretes data into an unreadable form. Normally only one security approach is used at a time by the users either cryptography or steganography. the combination of steganography and cryptography techniques are the most useful and powerful security techniques, also they can play a very important role in this field.

Basic Model: the basic steganography proposed model as shown in Figure 1 contains two files: First one is a cover image and Second is the secret file which will be hidden by a private key to encrypt the secret file. As shown in Figure 1 there are two steps, the first one hide data (embedding technique) and the other to compress it to reduce the spaces and the size of data. The end result of the system is the stego-image which is the digital image that has the secret message hidden interior. Stego-image is sent to the receiver via the public communication channel (internet) where the receiver will get the secret data out from the stego-image by applying an extracting set of rules with the secret password.

LSB Substitution: the LSB is one of the first useful coding techniques in steganography applications [3, 4].This method utilizes spatial embedding techniques and embeds the secret data into the cover image in which the pixels are subject to slight changes. Consequently, it's almost impossible for the Human Vision System (HVS) to notice by these slight changes so the

Received July 26, 2018; Revised January 31, 2019; Accepted February 27, 2019

possible adversary attacks will be decreased. Although this coding method integrates a simple tool in many packages, it cover ages some signs of weakness. Noise, filtering, clipping, color spatial transformations, and re-sampling are the weakest states of the LSB approach. Further, this approach can be affected by lossy compression algorithms in order that the extraction of the secret data cannot be assured in applications where compressed video streams are used.

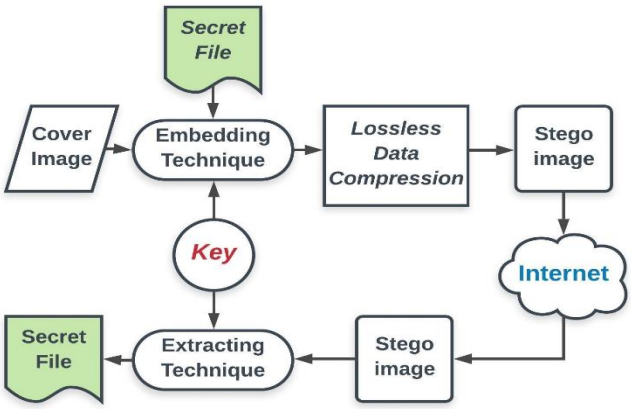

Figure 1. Basic model

The mathematical functions DCT is applied to transfer the digital image data from the spatial domain to the frequency domain. In DCT, after transforming the image within the frequency domain, the data is embedded inside the LSB of the medium frequency components and is detailed for lossy compression. DCT Technique coefficients are used for JPEG compression [5]. It divides the image into parts of differing importance. It transforms the image or a signal from the spatial domain to the frequency domain. It could discrete the image into high, middle and low frequency components, in low frequency sub-band, a lot of the signal energy lies at low frequency which contains most important visual parts of the image while in high frequency sub-band, high frequency components of the image are usually eliminated via compression and noise attacks. So the secret message is embedded by adjusting the coefficients of the middle frequency sub-band so that the visibility of the image will not be affected. The common equation for a 1D (N data items) DCT is defined by the following (1): [6, 7].

$$C(u) = a(u) + \sum_{i=0}^{n-1} \left(xi \cos \frac{\pi u(2i+1)}{2N} \right) \quad (1)$$

where u= 0, 1, 2… N-1. and The common equation for a 2D (NxM image) DCT is defined by the following (2):

$$C(u,v) = a(v) + \sum_{i=0}^{n-1} [a(u) \sum_{i=0}^{n-1} \left(xi \cos \frac{\pi u(2i+1)}{2N} \right)] * \cos \left(\frac{\pi v(2i+1)}{2N} \right) \quad (2)$$

where u, v = 0, 1, 2…. N-1. Here, the input image is of dimension N X M. c (i, j) is the depth of the pixel in row i and column j; C (u,v) is the DCT coefficient in row u and column v of the DCT matrix. DCT is used in steganography as 4- Image is broken into 8×8 blocks of pixels. Operating from left to right, top to bottom, DCT is applied to each block. Each block is compressed via quantization table to scale the DCT factors and message is embedded in DCT factors. For data reduction during the quantization phase, DCT factors are quantized by using the regular quantization table. The HVS is a great deal extra touchy to the values in low-frequency components than those in the higher frequencies. for this reason, distortion in high-frequency components is visually acceptable and perceptible [8-14].

Cryptography: cryptography is the art of complete the security by encoding the messages to mark them as non-readable. Cryptography is an act of transmitting the data safely

via the network and Internet by applying some cryptographic algorithms so that it will be hard for intruders to attack the confidential or private information. Two basic procedures used in cryptography are encryption and decryption; encryption procedure is the process of converting plain text into cipher text and decryption procedure is the reverse process of encryption. Plain text is the text which has the original message or data which is not encrypted and the ciphertext is the text which is ready to be used after the encryption of the message. A key is required for both the encryption and decryption of the data or message [15-20].

2. Related work

In this section, we briefly review the DCT transform and then introduce three selected DCT-based data hiding schemes: Iwata et al.'s data hiding scheme [5], Chang et al.'s [6] and Lin and Shiu's [7] reversible data hiding schemes. Discrete Cosine Transform (DCT) and Quantization. DCT is an extensively used mechanism for image transformation adopted to compress JPEG images [8]. within the JPEG compression procedure, which includes five phases: transforming an RGB image to a YCbCr image, composition of smallest coding units, two dimensional DCT, quantization of DCT coefficients, run length coding and Huffman coding. In the two dimensional DCT phase, each 8×8 non-overlapping block converted into Watermark inserted into DCT domain by using the two dimensional DCT Secret message from the public and private key. The sender generates the stego-image consistent with Embed algorithm DCT [9].

V.Santh et al. In that first odd price is chosen for watermark embedding in all special band after first stage decomposition [10]. A hybrid approach based on DCT and SVD is usually recommended. More transparency is obtained using only Odd values of a recognized pattern and LPSNR is adopted to obtain high robustness [11, 17]. The author recommended a watermarking scheme based on DCT-DWT-SVD. They apply second level decomposition of the cover image. DCT is applied to second level HL factor and divides it into four quadrants using zigzag series. SVD is applied to each quadrant and adjusted with SVD of the watermark. The algorithm gives appropriate PSNR and also robust to various attacks. Quadrant B1 gives properly consequences as compared to other three [12, 18]. The author proposed a watermarking scheme based totally on DWT and SVD using all four frequency bands. Singular values of Watermark are inserted into all four frequency bands singular values after first stage DWT. Experimental results show that LL gives the best magnitude of wavelet coefficient as well as of singular values [4, 19].

In [12] offered steganography technique that is based on block matching in DWT domain. By using naïve BM technique which develop the quality of the replicated secret image. In [7] offered steganography technique by implement a random key producer as a method. Stream cipher (LFSR) is the basic idea behind random key producer. Another thing which is use known beta that will importance on the choice of the cover image. In [13] offered steganography technique which is the combination of image steganography and cryptography. For Encrypt secrete data they used content based encryption technique and raster scan technique along with LSB is used for image steganography.

In [14], a method of hiding of data in Black and White images was suggested that used blocks to hide data rather than changing one or a pair of bits of pixels. A block of proper size 2*2, 3*3 is selected and maximum 2- pixels are changed in 3*3 block and only 1-pixel in 2*2 block to keep up visual quality of the image. An odd-even feature of blocks was used. Bit 1 is place in odd numbered blocks and bit 0 is place in even numbered blocks. Central pixel is used to checked whether bit is existing in that block or not.

A new steganographic algorithm for RGB images was offered in [15], where 2-different techniques namely, Matrix Pattern (MP) and LSB were combined. Spatial domain of images is used by these 2-techniques. In MP technique, covered image is divided into B×B blocks that are non-overlapping. Message is transformed into t1×t2 matrix patterns. Then, hidden data is inside 4^{th} through 7bits of blue channel in that covered image. In the offered algorithm, the message is hidden inside first 3-bit layers and 4^{th} to 7^{th} bit layer of RGB cover image combining LSB and MP methods. The results presented that this new policy has better capability than LSB and MP methods used separately. The stego-image has also a good PSNR value.

Most of the watermarking schemes noted above the gray scale image is used as a cover image and binary or grayscale watermark. In suggested scheme color image is used as a

cover image and a watermark image. Consequently, capacity is extended. To achieve robustness in opposition to specific attacks watermark is embedded inside the lower band and to get suitable transparency amendment is carried out in odd values. DCT gives the great result of compression therefore to overcome problems of compression attacks in existing techniques in second technique we practice DCT to both cover image as well as the watermark [16]. The results showed that the presented technique has better PSNR and payload capacity as well. This paper is ordered as follows, Section II, we argued the relevant research work of the data hiding based totally on compression strategies. Section III describes our counseled technique. Section IV shows the experimental results, and conclusions are given in Section V.

3. Proposed Algorithms

In the proposed technique, we applied multiple methods to hiding image by applying DCT algorithm to embed the image and encrypt the data via cryptography algorithms, applying DCT compression [21-25], then stego-image will transfer via the internet after that on the other side the reverse method will be performed on stego-image by decrypting it using the private key to extract the data. In the proposed algorithm, it is assumed that the sender as well as the receiver holds the same system of private keys. Indeed, the receiver sends the public key to the sender by an insecure communication channel. Then, the sender generates the stego-image with both keys and sends them through another insecure channel to the receiver, who can extract the secret file, which inserted into the cover image by the embedding procedure.

3.1. Embedding Algorithm

The embedding algorithm flowchart is shown in Figure 2, the steps of the algorithm are as the follows:

Input: (Cover image, Secret file, key)

The secret file is place in the cover image by the embedding procedure.

- Read cover image.
- Read secret Key.
- Read the secret file and convert it to binary.
- The cover image is dived into 8×8 block of pixels.
- DCT is applied to each block.
- Each block is compressed over and done with quantization table.
- Determine LSB of each DCT coefficient and replace with LSB of secret file.
- Write stego-image.
- Calculate the Mean Square Error (MSE) and Peak signal to noise ratio (PSNR) of the stego image.

3.2. Extracting Algorithm

The extracting algorithm flowchart is shown in Figure 3, the steps of the algorithm are as the follows:

Input: (Stego-image)

To extract image

- Read the stego image and Encrypted secret file which is to be hidden in it.
- Transform the stego image into binary.
- Get the horizontal and vertical filtering coefficients of the stego image. stego image is adde with data bits for DCT coefficients.
- Get stego-image.

Output : Stego-image before compress

To regain secret file

- Read secret Key.
- Find the horizontal and vertical filtering coefficients of the cover image. Extract the file bit by
- bit and recomposing the cover image.
- Transform the data into message vector and Compare it with the original file.
- Get secret file.

Output : (Cover image, secret file)

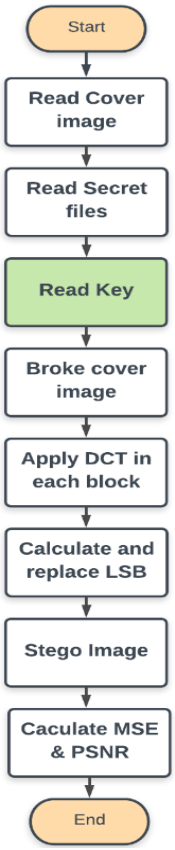

Figure 2. Flowchart of embedding Algorithm

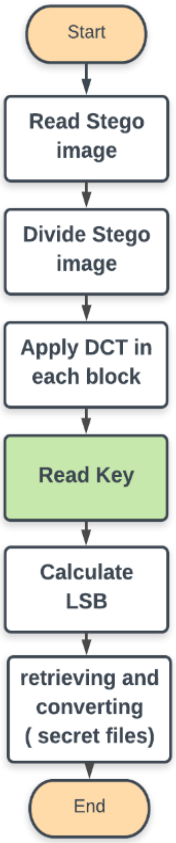

Figure 3. Flowchart of extracting Algorithm and retrieve secret message

4. Experimental Results

The experiment of using steganography in cover image is to hide as much data as possible with the lowest noticeable difference in the stego-image. As enactment measurement for image distortion, a practical objective measure for this property are the Mean Squared Error (MSE) and the Peak Signal to Noise Ratio (PSNR) between the cover image and the stego-image. Mean Square Error (MSE): It is the degree used to quantify the alteration between the preliminary and the distorted or noisy image. Mean Square Error is calculated using the following formula:

$$\text{MSE} = \frac{1}{mxn} \sum_{i=1}^{n-1} \sum_{j=0}^{n-1} (o\,(i.j) - s\,(i,j))^2 + (2n+m)$$

or

$$\text{MSE} = \frac{1}{mxn} \sum_{i=1}^{n-1} \sum_{j=0}^{n-1} (o\,(i.j) - s\,(i,j))^2 \quad (3)$$

where ‘‘S’’ and ‘‘O’’ are the stego-image and original image respectively to be compared and their image sizes are (m x n). where m and n are number of rows and columns.
we can find Peak Signal to Noise Ratio (PSNR) which measures the quality of the image by comparing the original image with the stego-image. PSNR is used to calculate the quality of the stego-image after embedding the secret message in the cover image.

$$\text{PSNR} = 10 \log_{10} \frac{256^2}{MSE} \quad (4)$$

where in 256 is the wide variety of bits that constitute a pixel within the image. as an example, The PSNR parameter is computed at the depth portion of the images. The number of faded bits

relies upon on hidden data capacity (HDC) and the perceptibility level. In truth, traditional PSNR measurements do no longer correspond to an individual's perception. PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values falling below 30 dB suggest a fairly low quality, i.e., distortion because of embedding can be obvious; however, a high-quality stego image should struggle for 40 dB and above. In this section, we report the experimental results evaluating our approach with the O.CETIIN et al. [16] schemes.

To expose the overall performance of the proposed algorithm, We implement the schemas proven by using O.CETIIN et al. [16], the proposed algorithm in this paper is using MATLAB software. The embedded image was created by repeat a predefine message until the embedded message with required length is generated. In Figure 4, We used 'Jet.jpg' and 'Baboon.jpg' as test cover image files from under MATLAB software toolbox folder and also Photos 'MidoToto.jpg' and 'MonaLisa.jpg'. We used PSNR (peak signal to noise ratio) to evaluate the distortion between the original image and Stego-image [17-27].

The proposed algorithm able to hide image based on two methods in DCT by embed and compress the image to hide and extract the secret messages, which mean hiding request data by minimizing the image size. From the gained results we can conclude that the embedding capacity in the proposed algorithm is very good and as shown in Table 1 which shows the results and Table 2 which shows the parameters analysis of LSB and DCT Methods. PSNR and MSE show that the image quality is high and has a higher level of security, in case of using DCT with LSB than using LSB alone which mean low distortion in the stego image. Moreover, the security is higher than using LSB alone.

Table 1. PSNR and MSE

Cover Image	LSB technique		DCT technique	
	PSNR (db)	MSE (db)	PSNR (db)	MSE (db)
MidoToto .jpg	49.732	1.302	60.454	0.977
Jet.jpg	48.867	1.371	55.56	0.895
Baboon.jpg	48.254	1.391	51.22	0.575
MonaLisa.jpg	48.980	1.402	53.42	0.678

Table 2. Parameters Analysis of LSB and DCT Methods

Features	LSB	DCT
Invisibility	Low	High
Cover image capacity	High	Meduim
Robustness against image manipulation	Low	Medium
PSNR	Medium	High
MSE	Medium	Low

Figure 4. Output of image embedding process:
(a) cover image (b) secret image (c) stego-image

5. Conclusion

The performance of a comparison between two different techniques is given. The first technique used LSB with no encryption and no compression. In the second technique, the secret message is encrypted first then LSB technique is applied. Moreover, DCT is used to transform the image into the frequency domain. According to results obtained in this paper, it is clear that we can hide the intended data in messages while minimizing its size, enabling us to transfer the data more securely with less overall burden in capacity in comparison to other algorithms.The performance of these two techniques is evaluated on the basis of the parameters MSE and PSNR. Using LSB and DCT effectively reduce the overall number of bits/bytes in a file so it can be transmitted faster over slower Internet connections, or take up less space on a disk. so our technique shows to be effective with keeps the criteria of perceptibility, capacity, and robustness of a standard steganographic algorithm.

References

[1] Aumreesh Kumar Saxena, Sitesh Sinha, Piyush Shukla. Design and Development of Image Security Technique by Using Cryptography and Steganography: A Combine Approach. *International Journal of Image, Graphics and Signal Processing*. 2018; 10(4): 13-21.

[2] Ismael Abdul Sattar, Methaq Talib Gaata. *Image steganography technique based on adaptive random key generator with suitable cover selection*. Annual Conference on New Trends in Information & Communications Technology Applications, Iraq. 2017: 208-212.

[3] Kelash HM, Osama F AbdelWahab, Elshakankiry OA. *Hiding Data in Video Sequences Using Steganography Algorithms*. ICT International Conference, IEEE. Jeju Island, Korea. 2013: 353-358.

[4] Emir Ganic, Ahmet M Eskicioglu. Robust DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies. MM&SEC'04. Magdeburg, Germany. 2004.

[5] M Iwata, K Miyake, A Shiozaki. Digital Steganography Utilizing Features of JPEG Images. *IEICE Trans. Fundamentals*. 2004; E87-A (4): 929–936.

[6] CC Chang, CC Lin, CS Tseng, WL Tai. Reversible hiding in DCT-based compressed images. Information Sciences. 2007; 177: 2768-2786.

[7] CC Lin, PF Shiu. *DCT-based reversible data hiding scheme*. Proc. of the 3rd International Conference on Ubiquitous Information Management and Communication. 2009: 327– 335.

[8] Md Khalid Imam Rahmani, KamiyaArora, Naina Pal. A Crypto-Steganography: A Survey in. *International Journal of Advanced Computer Science and Applications*. 2014; 5(7): 149-155.

[9] M Ghanbari. Editors. Standard Codecs: Image Compression to Advanced Video Coding. *IET*. 2004.

[10] Zhi-Hong Guan, Fangjun Huang. A hybrid SVD-DCT watermarking method based on LPSNR. Pattern Recognition Letters. *Elsevier*. 2004: 1769–1775.

[11] Srinivasa Kumar Devireddy, Nageswara Rao Thota. Image Compression Using Discrete Cosine Transform. *Georgian Electronic Scientific Journal*: *Computer Science and Telecommunications*. 2008; 17(3): 133-150.

[12] Jaeyoung Kim; Hanhoon Park; Jong-Il Park. *Image steganography based on block matching in DWT domain.* IEEE International Symposium on Broadband Multimedia Systems and Broadcasting. Italy. 2017: 1–4.

[13] Shivani Chauhan; Jyotsna; Janmejai Kumar; Amit Doegar. *Multiple Layer Text security Using variable block size cryptography and image steganography*. 3rd International Conference on Computational Intelligence & Communication Technology. India. 2017: 1-7.

[14] Nilchi, Amirfarhad Nilizadeh. *A novel Steganography method on Matrix Pattern and LSB algorithms in RGB Images*. 1st Conference on Swarm Intelligence and Evolutionary Computation. Iran. 2016: 154-159.

[15] P Venkateswaran, Souvik Roy. *Online Payment System using Steganography and Visual Cryptography*. Conference on Electrical, Electronics and Computer Science, IEEE. Bhopal, India. 2014: 101-115.

[16] AOZCERIT, OCETIIN. A new for Color Images, Proceedings of International Steganography Algorithm Based on Color Histograms for Data Embedding into Raw Video Streams. *Elsevier Ltd*, *Computers & Security*.Turkey. 2009; 28: 670-682.

[17] CH Yang, YC Lin. Fractal curves to improve the reversible data embedding for VQ-indexes based on locally adaptive coding. *J. Vis.Commun. Image Represent*. 2010; 21(4): 334–342.

[18] HW Tseng, CC Chang. High capacity data hiding in JPEG compressed mages. *Informatica*. 2004; 15(1): 127–142.

[19] A El_Rahman S. A comprehensive image steganography tool using LSB scheme*. Int J Image Graph Sig Process*. 2015; 7(6): 10–18.

[20] Elangovan B, Rajesh K, Venkateswari P. An efficient method for high secured image steganography using image segments. *Int J Appl Eng Res.* 2013; 8(12): 1449–57.

[21] Raja KB, Chowdary CR, Venugopal KR, Patnaik LM. *A secure image steganography using LSB, DCT and compression techniques on raw images*. In: 3rd international conference on intelligent sensing and information processing. 2005: 171–176.
[22] Suchitra B, Priya M, Raju J. Image steganography based on DCT algorithm for data hiding. *Int J Adv Res Comput Eng Technol.* 2013; 2(11): 3003–3006.
[23] Wafaa MA, Abdul Monem SR, Al-Sakib Kh P. Mix column transform based on irreducible polynomial mathematics for color image steganography: A novel approach. *Comput Electr Eng*. 2014; 40(4): 1390–404.
[24] Walia E, Jain P, Navdeep. An analysis of LSB & DCT based steganography. *Glob J Comput Sci Technol*. 2010; 10(1): 4–8.
[25] Singh PVT. Matlab implementation of baseline JPEG image compression using hardware optimized discrete cosine transform. *Int J Eng Sci Invent* 2014; 3(8): 47–53.
[26] Bansal D, Chhikara R. An improved DCT based steganography technique. *Int J Comput Appl*. 2014; 102(14): 46–49.
[27] Osama F, Abdel Wahab, Mohamed B Badawy, Hala S El-sayed. Utilizations of Reversible Lossless Data Hiding Techniques in Video Sequences. *International Journal of Computing and Network Technology*. Bahrain University. 2015; 3(1): 9-16.